Committee Secretary

Joint Standing Committee on Treaties

PO Box 6021

Parliament House

Canberra ACT 2600

By email: jsct@aph.gov.au

22 March 2022

Re: ***Agreement between the Government of Australia and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime***

Dear Committee Secretary,

I welcome the opportunity to provide this submission to the Parliamentary Joint Standing Committee on Treaties concerning the *Agreement between Australia and US on Access to Electronic Data for the Purpose of Countering Serious Crime* ('**CLOUD Act Treaty**'). I am a law student at the University of New South Wales.

This submission supports in principle the implementation of the CLOUD Act Treaty and its clarification of the international law on transborder data production orders. However, it recommends that the treaty's legal oversight mechanisms be improved.

Recommendations

1. The CLOUD Act Treaty should be adopted and binding treaty action should be taken, subject to the recommendations below.
2. The JSCOT should consider introducing an external dispute resolution clause into the CLOUD Act Treaty to safeguard human rights and the rule of law.
3. The CLOUD Act Treaty should be amended to require review of international production orders by a 'court, judge, or magistrate', deleting the indeterminate category of an 'other independent authority' in article 5(2).

Kind regards,

Henry Chen

Recommendation 1: The CLOUD Act Treaty should be adopted and binding treaty action should be taken, subject to the recommendations below.

The CLOUD Act Treaty addresses a major legal grey area on sovereignty in international law, enabling Australian law enforcement to more easily access stored computer data overseas using international production orders. An international agreement is preferable to relying on the alternatives of mutual legal assistance and voluntary disclosure.

Sovereignty – the default position

Under international law, a State may not exercise enforcement jurisdiction in the territory of another State unless there is a treaty or a customary rule that allows it to do so.[1] Enforcement jurisdiction refers to the performance of coercive governmental functions, such as making arrests, or conducting police or administrative investigations.

There is disagreement among international lawyers about whether issuing a transborder data production order is a prohibited exercise of extraterritorial enforcement jurisdiction. On one view, compelling a company in another State's territory to divulge private information stored overseas interferes with the sovereign law enforcement rights of that other State.[2] On the other hand, production orders may amount to a purely territorial exercise of jurisdiction because there is no direct extraterritorial enforcement by State organs, with all overseas acts being carried out by the foreign company.[3]

If international production orders are prohibited under international law by default, then their use is a breach of sovereignty and an internationally wrongful act. In this legal grey area, the *Budapest Convention on Cybercrime*, which Australia entered in 2013, provides little assistance. This treaty envisages mutual legal assistance and voluntary disclosure as the mechanisms for the lawful provision of overseas data to law enforcement.

Mutual legal assistance

[1] Michael Schmitt and Liis Vihul, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017) 66 ('Tallinn Manual'); *SS 'Lotus' (France v Turkey) (Judgment)* [1927] PCIJ (ser A) No 10, 18.
[2] Tallinn Manual 70. See *Microsoft Corporation v United States of America*, 829 F3d 197 (2d Circ 2016) 39–42 ('Microsoft Ireland case').
[3] Ibid; American Law Institute, *Restatement (Fourth) of the Foreign Relations Law of the United States* (2017) s 432; Jack Goldsmith, 'The Internet and the Legitimacy of Remote Cross-Border Searches' (University of Chicago Public Law & Legal Theory Working Paper No 16, 2001); Ahmed Ghappour, 'Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web' (2017) 69 *Stanford Law Review* 1075.

The *Budapest Convention* obliges States to cooperate in criminal investigations in cyberspace,[4] providing a uniform framework to supplement bilateral mutual assistance treaties. These treaties are enabled in Australia by the *Mutual Assistance in Criminal Matters Act 1987*.

However, these mutual assistance mechanisms have been widely observed to be inadequate. The Council of Europe's Convention on Cybercrime Committee noted in 2014 that:

> [t]he mutual legal assistance (MLA) process is considered inefficient in general, and with respect to obtaining electronic evidence in particular. Response times to requests of six to 24 months appear to be the norm. Many requests and thus investigations are abandoned. This adversely affects the positive obligation of governments to protect society and individuals against cybercrime and other crime involving electronic evidence.[5]

In Australia, the Department of Home Affairs notes that data requests to companies like Google and Facebook 'can take 12 months or longer', as United States authorities must review the requests and seek domestic warrants.[6] In these circumstances, there is a demonstrated need for the international production order regime. Australia made some 1000 mutual assistance requests to the United States seeking data from communications service providers between 2007 and 2020.[7] Fewer than 30 such requests were made by the US to Australia in the same time period.[8]

Voluntary disclosure

Article 32(b) of the *Convention on Cybercrime* permits States to access data stored overseas with the 'lawful and voluntary consent of the person who has the lawful authority to disclose the data'.

Given the inefficiency of mutual legal assistance, States have turned to making direct voluntary requests to overseas service providers for data production. However, where States do not have the legal ability to compel foreign companies to give data to law enforcement, their investigative capabilities are determined by 'bargaining' and 'political massage' with these

[4] *Convention on Cybercrime* (23 November 2001) ETS 185 arts 24–35.
[5] Cybercrime Convention Committee (T-CY), 'T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime adopted by the T-CY at its 12th Plenary (2–3 December 2014)' (2014) 123.
[6] Department of Home Affairs, 'Regulation Impact Statement for the Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime' 3–4.
[7] Ibid 3.
[8] Ibid 8.

companies.[9] This creates a significant risk that State practice will be determined by the individual discretions of rank-and-file officers and the commercial interests of multinational corporations, sidelining the sovereign rights of States.[10]

In any event, the company targeted by the order may be subject to conflicting domestic legal obligations to refrain from disclosing data, known as 'blocking statutes'.[11] Thus, irrespective of the international law position, service providers may be placed in an impossible dilemma, as occurred in the *Microsoft Ireland* case.

Consent and reciprocity framework – CLOUD Act Treaty

The CLOUD Act Treaty provides a principled resolution to the murky state of international law on extraterritorial warrants. It enables States to lay down clear and binding legal rules for the provision of data by overseas service providers to law enforcement.

The terms of the CLOUD Act Treaty maintain State consent and governmental legitimacy as the basis for setting aside the ordinary sovereignty rule. Disputes between Australian service providers and the US government are conclusively resolved by the unilateral decision of Australia's Designated Authority, and vice versa.[12] The CLOUD Act Treaty also provides for periodic review and consultation between the parties to ensure that its purpose and provisions are being fulfilled.[13]

For this reason, arguments by industry players that civil penalties are contrary to the spirit of the CLOUD Act Treaty are misplaced.[14] The consent-based framework of the CLOUD Act Treaty enables States to determine their own rules for the provision of data, and intentionally takes those decisions out of the hands of corporations like Google and Facebook.

---

[9] Paul de Hert, Cihan Parlar and Johannes Thumfart, 'Legal arguments used in courts regarding territoriality and cross-border production orders: From Yahoo Belgium to Microsoft Ireland' (2018) 9(3) *New Journal of European Criminal Law* 326, 328–329.

[10] Ahmed Ghappour, 'Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web' (2017) 69 *Stanford Law Review* 1075.

[11] In Australia, these obligations are now excluded by Part 13 of Schedule 1 of the *Telecommunications (Interception and Access) Act*. In the United States, these obligations are excluded by section 104 of the *CLOUD Act*.

[12] *CLOUD Act Treaty* art 5(12).

[13] *CLOUD Act Treaty* art 11(1).

[14] Google, Submission No 21 to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Telecommunications Legislation Amendment (International Production Orders) Bill 2020* (30 April 2020) 2.

Recommendation 2: The JSCOT should consider introducing an external dispute resolution clause into the CLOUD Act Treaty to safeguard human rights and the rule of law.

The consent-based approach to international cooperation is taken too far in Article 11(2) of the CLOUD Act Treaty, which explicitly excludes external dispute resolution between Australia and the United States:

> The Parties may consult at other times as necessary or to resolve disputes concerning the implementation of this Agreement, and any such disputes shall not be referred to any court, tribunal, or third party.

Under the CLOUD Act Treaty there is a risk that situations will arise, particularly in relation to the US death penalty, where the United States' compliance with the procedures in the CLOUD Act Treaty may be a significant issue. Past submissions to the PCJIS have observed that any treaty Australia enters under the international production orders framework must contain substantive protections for human rights.[15] This is because the framework for incoming orders in Part 13 of Schedule 1 of the *Telecommunications (Interception and Access) Act 1979* is entirely permissive. While outgoing orders are subject to Australian domestic legal protections, incoming orders are not.

The absence of external dispute resolution is particularly problematic in light of the United States' poor record on transparency and whistleblower protection. The United States has engaged in unlawful mass surveillance against its own citizens,[16] and continues to prosecute the Australian citizen and Wikileaks founder Julian Assange for espionage.[17] As incoming orders under the CLOUD Act Treaty are made directly to service providers,[18] the Australian government will have no oversight of these orders. Instead, it is left entirely up to Australian companies to challenge the legality of orders made against them by the United States.

---

[15] Australian Privacy Foundation, Submission No 1 to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Telecommunications Legislation Amendment (International Production Orders) Bill 2020* (1 April 2020); Australian National University Law Reform and Social Justice Research Hub, Submission No 17 to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Telecommunications Legislation Amendment (International Production Orders) Bill 2020* (30 April 2020).
[16] Raphael Slatter, 'U.S. court: Mass surveillance program exposed by Snowden was illegal', *Reuters*, 3 September 2020, <https://www.reuters.com/article/us-usa-nsa-spying-idUSKBN25T3CK>.
[17] Ben Quinn, 'Julian Assange can be extradited to US to face espionage charges, court rules', *Guardian*, 11 December 2021, <https://www.theguardian.com/media/2021/dec/10/julian-assange-can-be-extradited-to-us-to-face-espionage-charges-court-rules>.
[18] *CLOUD Act Treaty* art 5(5).

While the text of the CLOUD Act Treaty contains numerous protections for human rights and non-discrimination,[19] the absence of a dispute resolution mechanism means that Australia has few binding remedies available if the United States exceeds its powers. For example, if the United States targets Australians with data production orders, or improperly uses Australian data in a death penalty case, Australia's only options will be to do nothing, or to terminate the treaty with one month's notice[20] and lose the benefit of the data production order regime.

Bilateral treaties do sometimes omit external dispute resolution, as 'rational states will not pay costs if such provisions are unlikely to be used'.[21] However, while many bilateral treaties are silent on the point, it is rare for external dispute resolution to be entirely excluded.[22] Recent Australian bilateral treaties with Timor-Leste on air services[23] and with the United Kingdom on nuclear energy cooperation[24] have included binding dispute resolution mechanisms through referral to arbitral tribunals. Similarly, Australia's mutual legal assistance treaty with Switzerland allows disputes to be referred to the International Court of Justice.[25] Such provisions could easily be included in the CLOUD Act Treaty.

[19] *CLOUD Act Treaty* arts 3(4), 3(5), 4(1), 4(2), 5(1), 7, 9.
[20] *CLOUD Act Treaty* art 16(2).
[21] Barbara Koremenos, 'If Only Half of International Agreements Have Dispute Resolution Provisions, Which Half Needs Explaining?' (2007) 36(1) *Journal of Legal Studies* 189, 209–210.
[22] For an example of exclusion, see *Treaty between the Government of Australia and the Government of Malaysia on Mutual Assistance in Criminal Matters* (28 December 2006) ATS 21, art 25.
[23] Agreement between the Government of Australia and the Government of the Democratic Republic of Timor-Leste relating to Air Services (19 May 2021) ATS 9, art 17.
[24] *Agreement between the Government of Australia and the Government of the United Kingdom of Great Britain and Northern Ireland on Cooperation in the Peaceful Uses of Nuclear Energy* (1 January 2021) ATS 1, art XVIII.
[25] *Treaty between Australia and Switzerland on Mutual Assistance in Criminal Matters* (31 July 1994) ATS 7, art 21.

Recommendation 3: The CLOUD Act Treaty should be amended to require review of international production orders by a 'court, judge, or magistrate', deleting the indeterminate category of an 'other independent authority' in article 5(2).

Numerous submissions to the PCJIS review of the CLOUD Act Treaty's enabling legislation[26] have raised concerns about the role and independence of the Administrative Appeals Tribunal ('**AAT**') in approving outgoing production orders. The PCJIS waved away these concerns,[27] uncritically adopting the Department of Home Affairs' position that the Australian legislation 'facilitates' the US CLOUD Act's requirement of 'authorisation of orders by persons characterised as a court, judge, magistrate or other independent authority'. This statement in the US legislation has been incorporated into article 5(2) of the CLOUD Act Treaty.

The current CLOUD Act Treaty framework, where politically appointed AAT members[28] can approve data production orders in criminal investigations, risks leaving Australia with a second-class system. Although judicial review is theoretically available against such AAT decisions, investigation suspects targeted by data production orders will not ordinarily be aware of the orders until after they are made, as there is no notification requirement. By contrast, EU law requires systematic and prior judicial authorisation for the issuing of investigative measures, making it likely that a future US-EU CLOUD Act Treaty will require judicial approval.[29]

The CLOUD Act Treaty recognises that international production orders are significant enough to be limited to investigations of 'serious crimes' with a maximum penalty of at least three years' imprisonment.[30] This is the basis for departing from the ordinary rules of sovereignty and mutual legal assistance, allowing orders to be sent directly to overseas service providers, with no notice to foreign governments. Given the treaty's recognition of the seriousness of such orders, the CLOUD Act Treaty should require prior judicial oversight of international production orders.

---

[26] Telecommunications Legislation Amendment (International Production Orders) Bill 2021 (Cth).
[27] Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Telecommunications Legislation Amendment (International Production Orders) Bill 2020*, 60–63.
[28] Mike Seccombe, 'Political stacking leaves appeals tribunal in chaos', *Saturday Paper*, 24 November 2018, <https://www.thesaturdaypaper.com.au/news/politics/2018/11/24/political-stacking-leaves-appeals-tribunal-chaos/15429780007187>.
[29] Sergio Carrera et al, 'Cross-border data access in criminal proceedings and the future of digital justice' (Centre for European Policy Studies, October 2020) 35.
[30] *CLOUD Act Treaty* art 1(15).